Claims

What is claimed is:

1. A system for ciphering data stored within a memory buffer comprising:
an integrated processor for retrieving data from the memory buffer, for ciphering the data, and for performing operations relating to verification of data integrity, the ciphering and the performed operations executed in parallel, the processor for providing processed data

2. A system as defined in claim 1 comprising means for storing the processed data in the memory buffer.

3. A system as defined in claim 2 comprising a controller forming part of the integrated processor and for controlling operations of the integrated processor.

4. A system as defined in claim 3 wherein the processor comprises encryption means for ciphering the data and hashing means for performing operations relating to verification of data integrity.

5. A system as defined in claim 3 wherein the processor comprises encryption means for ciphering the data and digesting means for performing operations relating to verification of data integrity.

6. A system as defined in claim 4 wherein the encryption means includes a DES encryption means for performing one of DES and triple-DES encryption.

7. A system as defined in claim 4 wherein the hashing means comprises HMAC hashing means for encoding data integrity verification information within the data.

8. A system for ciphering data comprising:
a memory buffer having a first port and a second port;

a plurality of communication ports;

a first processor in communication with the first port of the memory buffer and the plurality of communication ports;

a second processor in communication with the second port of the memory buffer, the second processor for ciphering data within the memory buffer and for storing the data ciphered data within the memory buffer,

wherein data ciphering operations do not affect operations of the first processor.

9. A system as defined in claim 8 wherein the memory buffer comprises dual port random access memory.

10. A system as defined in claim 8 wherein the second processor comprises hash means for performing operations relating to verification of data integrity.

11. A system as defined in claim 8 comprising a data bus, wherein the first processor, the first port of the dual ported RAM, and some of the plurality of communication ports are all in communication through the bus.

12. A system as defined in claim 11 wherein the second processor is isolated from the bus by the dual ported RAM.

13. A system as defined in claim 8 wherein the first processor and the second processor operate asynchronously one to the other.

14. A system as defined in claim 13 wherein the first processor and the second processor are clocked by different clock sources that are asynchronous one to the other.

15. A system as defined in claim 8 wherein the second processor comprises means for retrieving a security context from memory, the security context for use in ciphering data.

16. A system as defined in claim 15 wherein the first processor comprises means for determining a security context relating to at least one of a source and a destination of data

packets and for storing the determined security context in memory accessible by the second processor.

17. A system as defined in claim 16 wherein first processor comprises means for storing an address based on the at least one of a source and a destination in memory in association with the determined security context.

18. A system as defined in claim 15 wherein second processor comprises means for providing an indication to the first processor when a security context is not present in memory.

add Ba

Add 5